

# Don't turn off Twitter and Facebook during unrest - turn them back on the rioters

Clive Longbottom, Service Director

## Quocirca Comment

---

As the politicians continue to argue over the causes of the riots that hit the UK in early August 2011, much pontificating has gone on about the role that Blackberry Messenger (BBM), Twitter and Facebook played in the events.

It is apparent that those behind the riots came from a mix of backgrounds and that the main cause of the unrest had little to do with the death of Mark Duggan. Out and out greed was the order of the day. Sure, there were individuals who if they had spent a few minutes reflecting on what they were thinking of doing would not have done it, and "sheep" who just followed others blindly. Some of these individuals even used the social networking sites to either tell others to join in or to boast of what they had done after the event.

But the main problem seems to be where real criminal forces were at work – the criminal gangs which are continually looking for situations which they can use, bringing the individuals in to their plans as smokescreens to the bigger picture. The riots were highly organised at a core level – and it is certain that social networking was used as a means of coordinating how the looting could be carried out to provide the best overall haul for the gangs themselves.

A host of politicians, mostly removed from the real world, have called for emergency services to have the capability to require those companies running social networking sites to shut them down during such uprisings in the future in order to prevent them being used to stir up the unrest. This is plainly unworkable. For a start, the rioters during the French Revolution of the late 18th century did not have "les mures" (Blackberries), or the capability to "ecrire sur le mur" in "la tete livre". Likewise, the Notting Hill

race riots in 1958, the Toxteth riots in 1981 and the many other riots that have occurred in the UK during the 1950s, 60s, 70s and 80s had no help from such technology. And what do you shut down? Facebook, Twitter, BBM are obvious targets. LinkedIn? MySpace? SecondLife? Microsoft Messenger? Maybe just turn off the Internet for a few days and hope that will cure all ills?

Agreed, technology can make things easier for the miscreants – a simple message can reach more people than something requiring phone calls or hand written messages. However, the power of cascade messaging cannot be overlooked – if I say something to two people, and they repeat it to two more each, who repeat it to two more, then after 26 retellings, the whole of the UK could know the message. Those planning something like this will not let the absence of social networks get much in their way.

What the politicians should be doing is looking far more at both the positives of social networking in these circumstances and the opportunities.

In the positive column has to go how the general population was kept updated on what was happening, and how many innocent people managed to keep away from hotspots due to being pre-warned of problems by others, well before any standard media outlets could issue such warnings. Next, those who needed help could use the sites to ask for the help – and many people found that their local communities pulled together during the riots through messages having been seen on social networks. After the riots, the way that Facebook and Twitter were used in order to organise clean up

groups and to show those who had been sucked into the riots that what they had done was wrong was great to see – the coming together of a greater community based around the concept of the global village.

In the opportunities column has to be that if these sites are being used by the people aggravating the disturbances, then the intelligence services should be using the sites as much (if not more) than everyone else. Much has been said about how the more organised parts of the riots were based on guerrilla tactics – the coming together of groups that knew how long they should stay in one place before dispersing and coming back together some time later elsewhere, so making it difficult for the police to try and second guess what was happening, and where it would be occurring.

A lot of the information was in the open, available for the police to see along with everyone else. Some would be in more closed groups involving loose affiliations of “friends” on Facebook and Twitter – but not secure in an informational sense. If the police had access to these feeds based on knowledge of who the ringleaders were, they could have assigned their forces accordingly and stopped the riots before they began.

This leaves us with BBM – a closed secure system where the police will have to look to the politicians to enable them to gain access to information as necessary. In essence, this is no different to what has been done for years –

phone taps need judicial sign-off, and private social networking tapping should need the same, but RIM should be able to provide access to its systems where a legal request requires it. If the UK does not have the skills within its intelligence services for this, then there should be a rapid training program. The new millennials coming through have the basic knowledge on how social networking is used in many different scenarios – train them in how to use pattern matching technologies and so on and the social networks can become as much a positive intelligence source as a negative environment for the criminal gangs to organise their activities.

Trying to cut off social networking during unrest is not only impractical, it is technically implausible, as identifying all possible means of social networking in a dynamic environment will just result in the use of sites hosted in countries where the UK has no jurisdiction. As citizens and politicians alike have applauded how social networking has been used during the Arab Spring, and have decried the crackdowns on such use in more repressive regimes, politicians pushing for repressive powers put the UK well onto the debit side of the freedom of speech list.

Not only could a highly publicised approach mean that the individuals would think twice before using social networks to try and foment bad behaviour, but it could also lead to the identification and capture of more of the organised crime bosses and gang leaders operating in the UK.

*This article first appeared on Silicon*  
<http://www.silicon.com>

## About Quocirca

Quocirca is a primary research and analysis company specialising in the business impact of information technology and communications (ITC). With world-wide, native language reach, Quocirca provides in-depth insights into the views of buyers and influencers in large, mid-sized and small organisations. Its analyst team is made up of real-world practitioners with first-hand experience of ITC delivery who continuously research and track the industry and its real usage in the markets.

Through researching perceptions, Quocirca uncovers the real hurdles to technology adoption – the personal and political aspects of an organisation's environment and the pressures of the need for demonstrable business value in any implementation. This capability to uncover and report back on the end-user perceptions in the market enables Quocirca to advise on the realities of technology adoption, not the promises.

Quocirca research is always pragmatic, business orientated and conducted in the context of the bigger picture. ITC has the ability to transform businesses and the processes that drive them, but often fails to do so. Quocirca's mission is to help organisations improve their success rate in process enablement through better levels of understanding and the adoption of the correct technologies at the correct time.

Quocirca has a pro-active primary research programme, regularly surveying users, purchasers and resellers of ITC products and services on emerging, evolving and maturing technologies. Over time, Quocirca has built a picture of long term investment trends, providing invaluable information for the whole of the ITC community.

Quocirca works with global and local providers of ITC products and services to help them deliver on the promise that ITC holds for business. Quocirca's clients include Oracle, Microsoft, IBM, O2, T-Mobile, HP, Xerox, EMC, Symantec and Cisco, along with other large and medium sized vendors, service providers and more specialist firms.

Full access to all of Quocirca's public output (reports, articles, presentations, blogs and videos) can be made at <http://www.quocirca.com>